

Daily brief, Tuesday, October 13, 2026

Oct 12, 8:00 PM to Oct 13, 8:00 PM ET

Generated Oct 31, 2026, 6:12 AM ET

0

Breaking

2

Newly exploited

0

Exploit code

48

Critical CVEs

1

Ransomware posts

0

New breaches

2 newly exploited, 48 new critical CVEs, 1 ransomware posts.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.8

CVE-2026-96951 Microsoft Windows CISA KEV

An unauthorized attacker bypasses a security feature on Microsoft Windows over a network.

8.6

CVE-2026-104935 Ivanti Connect Secure CISA KEV DETECTION

An attacker bypasses authentication and accesses sensitive data on Ivanti Connect Secure.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

48

10.0

CVE-2026-97229 GitLab GitLab KEV EXPLOIT CODE

An attacker can execute arbitrary code on the GitLab server without authentication.

9.8

CVE-2026-83693 Microsoft windows 10 1607

+2 more CVEs in the same release

An unauthorized attacker can execute code over a network on Windows 10 1607.

9.8

CVE-2026-70147 Microsoft windows 10 1607

+1 more CVEs in the same release

An unauthorized attacker can execute code over a network on Windows 10 1607.

9.8

CVE-2026-83578 Microsoft windows 10 1607

An unauthorized attacker can execute code over a network on Windows 10 1607.

9.8	CVE-2026-70157 Microsoft windows 10 1607 An unauthorized attacker can execute code over a network on Windows 10 1607.
9.8	CVE-2026-83517 Microsoft windows 10 1607 An attacker can execute code over a network on Microsoft Windows 10 1607.
9.8	CVE-2026-83782 Microsoft Windows 10 Version 1607 An unauthorized attacker can execute code over a network on Microsoft Windows 10 Version 1607.
9.8	CVE-2026-105010 Microsoft windows 10 1607 An attacker can elevate privileges on Microsoft's Windows 10 1607.
9.8	CVE-2026-69634 Microsoft windows 10 1607 An attacker can execute arbitrary code on Microsoft's Windows 10 1607.
9.8	CVE-2026-69639 Microsoft windows 10 1809 An attacker can execute arbitrary code on Microsoft's Windows 10 1809.
9.8	CVE-2026-104252 Linuxfoundation vitess An attacker can inject malicious JavaScript on Linuxfoundation's Vitess.
9.9	CVE-2026-109412 Ivanti Neurons Patch for Intune An attacker gets sensitive authentication information from Ivanti Neurons Patch for Intune with authentication.
9.0	CVE-2026-105008 Microsoft windows 10 1607 An unauthorized attacker can perform spoofing over a network using Windows Schannel.
9.8	CVE-2026-85928 Microsoft windows 10 1607 An unauthorized attacker can execute code over a network on Windows 10 1607.
9.4	CVE-2026-106173 Fortinet FortiSIEM DETECTION An attacker can execute unauthorized code or commands in FortiSIEM.
9.6	CVE-2026-110136 Google Chrome A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
9.9	CVE-2026-89107 SAP SE SAP S/4HANA (Manage Substitution/Validation Rules) An attacker gets arbitrary code execution in SAP S/4HANA (Manage Substitution/Validation Rules) with authentication.
10.0	CVE-2026-89111 SAP SE SAP Cloud The SAP Cloud SDK for Python contains an OAuth2 SSRF vulnerability affecting multi-tenant BTP applications. An attacker who controls the tenant_subdomain parameter can redirect OAuth2 token requests to an attacker-controlled server, causing client credentials
9.6	CVE-2026-109708 Mozilla Firefox A remote attacker can escape the sandbox in Mozilla Firefox.

9.9**CVE-2026-89110** SAP SE SAP NetWeaver Visual Composer

An attacker with low privileges gets internal operations in SAP NetWeaver Visual Composer.

25 more critical CVEs in this window: see the dashboard

Ransomware

1

1 victims posted to leak sites. Most active: qilin (1).

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. CVE IDs link to the full record on Watch Floor.